

KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN 249203)
ak@kazlg.com
Mona Amini (SBN 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff
Judy Kisling

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

JUDY KISLING, on behalf of herself
and all others similarly situated,

Plaintiff,

vs.

SAGE HOME LOANS
CORPORATION f/k/a LENOX
FINANCIAL MORTGAGE
CORPORATION d/b/a WESLEND
FINANCIAL INSURANCE
SERVICES, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

//

//

//

//

//

//

//

//

//

1 Plaintiff Judy Kisling (“Plaintiff”), individually and on behalf of all similarly
2 situated persons, alleges the following against Sage Home Loans Corporation f/k/a
3 Lenox Financial Mortgage Corporation d/b/a Weslend Financial Insurance Services,
4 Inc. (“Defendant”) based upon personal knowledge with respect to herself and on
5 information and belief derived from, among other things, investigation by her counsel
6 and review of public documents as to all other matters:

7 INTRODUCTION

8 1. Plaintiff brings this class action against Defendant for its failure to
9 properly secure and safeguard Plaintiff’s and other similarly situated current and
10 former Defendant’s customers’ and employees’ (collectively defined herein as the
11 “Class” or “Class Members”) personally identifiable information (“PII”), including
12 name, date of birth, passport number, driver’s license number, federal identification
13 number, state identification number, tax identification number, Social Security
14 information, financial account information, phone number, physical address, and
15 email address (collectively, “Private Information”) from cybercriminals.

16 2. On or about December 19, 2023, Defendant learned that an unauthorized
17 entity had gained access to consumer information on one of its computer servers. In
18 response, Defendant launched an investigation that revealed that an unauthorized
19 party had access to certain customer and employee files on the server on an
20 undisclosed date (the “Data Breach”).

21 3. As a result of the Data Breach, and in light of their Private Information
22 now being in the hands of cybercriminals, Plaintiff and Class Members were, and
23 continue to be, at significant risk of identity theft and various other forms of personal,
24 social, and financial harm. This substantial and imminent risk will remain for their
25 respective lifetimes.

26 4. Armed with the Private Information accessed in the Data Breach, the
27 cybercriminals who carried out the Data Breach can and will commit a variety of
28 crimes, including, *e.g.*, opening new financial accounts in Class Members’ names,

1 taking out loans in Class Members' names, using Class Members' names to obtain
2 medical services, using Class Members' information to obtain government benefits,
3 filing fraudulent tax returns using Class Members' information, obtaining driver's
4 licenses in Class Members' names, and giving false information to police during an
5 arrest or criminal investigation.

6 5. There has been no assurance offered by the Defendant that all personal
7 data or copies of data have been recovered or destroyed, or that it has adequately
8 enhanced its data security practices sufficiently to avoid a similar breach of its
9 network in the future.

10 6. Therefore, Plaintiff and Class Members have suffered and are at an
11 imminent, immediate, and continuing increased risk of suffering, ascertainable losses
12 in the form of harm from identity theft and other fraudulent misuse of their Private
13 Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred
14 to remedy or mitigate the effects of the Data Breach, and the value of their time
15 reasonably incurred to remedy or mitigate the effects of the Data Breach.

16 7. Plaintiff brings this class action lawsuit to address Defendant's
17 inadequate safeguarding of Class Members' Private Information that it collected and
18 maintained.

19 8. The potential for improper disclosure and theft of Plaintiff's and Class
20 Members' Private Information was a known risk to the Defendant, and thus
21 Defendant was on notice that failing to take necessary steps to secure the Private
22 Information left it vulnerable to an attack.

23 9. Upon information and belief, Defendant failed to properly monitor and
24 implement adequate data security practices with regard to its computer network and
25 systems that housed Plaintiff's and Class Members' Private Information. Had
26 Defendant properly monitored its networks and implemented adequate data security
27 practices, it could have prevented the Data Breach or, at the very least, discovered the
28 Data Breach sooner.

11. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and exfiltrated during the Data Breach.

PARTIES

12. Plaintiff Judy Kisling is, and at all times mentioned herein was, an individual citizen of the State of Oklahoma residing in Sawyer, Oklahoma.

13. Defendant, Sage Home Loans Corporation f/k/a Lenox Financial Mortgage Corporation d/b/a Weslend Financial Insurance Services, Inc., is a corporation incorporated in California, with an office and/or principal place of business located at 200 Sandpointe Avenue, 8th Floor, Santa Ana, California 92707.

JURISDICTION AND VENUE

14. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

15. This Court has jurisdiction over Defendant because it is incorporated in California, regularly conducts business in California, and has sufficient minimum contacts in California.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District, and Defendant maintains a principal place of business in this District.

FACTUAL ALLEGATIONS

Defendant's Collection of Plaintiff's and Class Members' Private Information

17. Defendant is a financial services company with a focus on mortgage lending.¹

18. As a condition of receiving mortgage lending services from and/or being employed with the Defendant, customers and employees are required to entrust it with highly sensitive personal information.

19. Thus, due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its customers and employees, Defendant promises to, among other things, keep their Private Information private; comply with industry standards related to data security and the maintenance of their Private Information; inform its customers and employees of its legal duties relating to data security and comply with all federal and state laws protecting their Private Information; only use and release customers' and employees' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers and employees if their Private Information is disclosed without authorization.

20. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

21. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

¹ *About*, SAGE HOME LOANS, <https://www.sagehomeloans.com/about> (last visited May 2, 2024).

The Data Breach and Defendant's Inadequate Notice

22. According to Defendant's Notice, it learned of unauthorized access to its computer systems on or around December 19, 2023, with such unauthorized access having taken place on or around December 5, 2023.

23. On or about February 2, 2024, Defendant customers and employees began receiving their notices of the Data Breach informing them that its investigation determined that their Private Information was exposed.

24. Defendant delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "security incident."

25. The notice letter then listed time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing only twelve (12) months of credit monitoring and insurance reimbursement policy, Defendant offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, Defendant sent a similar generic letter to all other individuals affected by the Data Breach.

26. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

27. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

28. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

29. Defendant knew or should have known that its electronic records would

1 be targeted by cybercriminals.

2 ***Defendant Failed to Comply with FTC Guidelines***

3 30. The Federal Trade Commission (“FTC”) has promulgated numerous
4 guides for businesses which highlight the importance of implementing reasonable
5 data security practices. According to the FTC, the need for data security should be
6 factored into all business decision making. Indeed, the FTC has concluded that a
7 company’s failure to maintain reasonable and appropriate data security for
8 consumers’ sensitive personal information is an “unfair practice” in violation of
9 Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g.,*
10 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

11 31. In October 2016, the FTC updated its publication, *Protecting Personal*
12 *Information: A Guide for Business*, which established cybersecurity guidelines for
13 businesses. The guidelines note that businesses should protect the personal customer
14 information that they keep, properly dispose of personal information that is no longer
15 needed, encrypt information stored on computer networks, understand their network’s
16 vulnerabilities, and implement policies to correct any security problems. The
17 guidelines also recommend that businesses use an intrusion detection system to
18 expose a breach as soon as it occurs, monitor all incoming traffic for activity
19 indicating someone is attempting to hack into the system, watch for large amounts of
20 data being transmitted from the system, and have a response plan ready in the event
21 of a breach.

22 32. The FTC further recommends that companies not maintain PII longer
23 than is needed for authorization of a transaction, limit access to sensitive data, require
24 complex passwords to be used on networks, use industry-tested methods for security,
25 monitor the network for suspicious activity, and verify that third-party service
26 providers have implemented reasonable security measures.

27 33. The FTC has brought enforcement actions against businesses for failing
28 to adequately and reasonably protect customer data by treating the failure to employ

1 reasonable and appropriate measures to protect against unauthorized access to
2 confidential consumer data as an unfair act or practice prohibited by the FTCA.
3 Orders resulting from these actions further clarify the measures businesses must take
4 to meet their data security obligations.

5 34. As evidenced by the Data Breach, Defendant failed to properly
6 implement basic data security practices. Defendant's failure to employ reasonable
7 and appropriate measures to protect against unauthorized access to Plaintiff's and
8 Class Members' Private Information constitutes an unfair act or practice prohibited
9 by Section 5 of the FTCA.

10 35. Defendant was at all times fully aware of its obligation to protect the
11 Private Information of its customers and employees yet failed to comply with such
12 obligations. Defendant was also aware of the significant repercussions that would
13 result from its failure to do so.

14 ***Defendant Failed to Comply with Industry Standards***

15 36. As noted above, experts studying cybersecurity routinely identify
16 businesses as being particularly vulnerable to cyberattacks because of the value of the
17 Private Information which they collect and maintain.

18 37. Some industry best practices that should be implemented by businesses
19 dealing with sensitive PII like Defendant include but are not limited to: education of
20 all employees, strong password requirements, multilayer security including firewalls,
21 anti-virus and anti-malware software, encryption, multi-factor authentication, backing
22 up data, and limiting which employees can access sensitive data. As evidenced by the
23 Data Breach, Defendant failed to follow some or all of these industry best practices.

24 38. Other best cybersecurity practices that are standard in the industry
25 include: installing appropriate malware detection software; monitoring and limiting
26 network ports; protecting web browsers and email management systems; setting up
27 network systems such as firewalls, switches, and routers; monitoring and protecting
28

physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

39. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

40. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Defendant Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

41. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

42. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect customer and employee Private Information;

- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to sufficiently train its employees regarding the proper handling of customer and employee Private Information;
- e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA; and
- f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

43. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

44. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

45. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with the Defendant.

//

//

//

//

//

//

Defendant Should Have Known that Cybercriminals Target PII to Carry Out Fraud and Identity Theft

46. The FTC hosted a workshop to discuss “informational injuries,” which are injuries that individuals like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.² Exposure of highly sensitive personal information that an individual wishes to keep private may cause harm to that individual, such as the ability to obtain or keep employment. Consumers’ loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

47. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims’ identities in order to engage in illegal financial transactions under the victims’ names.

48. Because a person’s identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to

² *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), available at https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_report_-_oct_2018_0.pdf (last visited on April 10, 2024).

1 manipulate individuals into disclosing additional confidential or personal information
2 through means such as spam phone calls and text messages or phishing emails.

3 49. In fact, as technology advances, computer programs may scan the
4 Internet with a wider scope to create a mosaic of information that may be used to link
5 compromised information to an individual in ways that were not previously possible.
6 This is known as the “mosaic effect.” Names and dates of birth, combined with
7 contact information like telephone numbers and email addresses, are very valuable to
8 hackers and identity thieves as it allows them to access users’ other accounts.

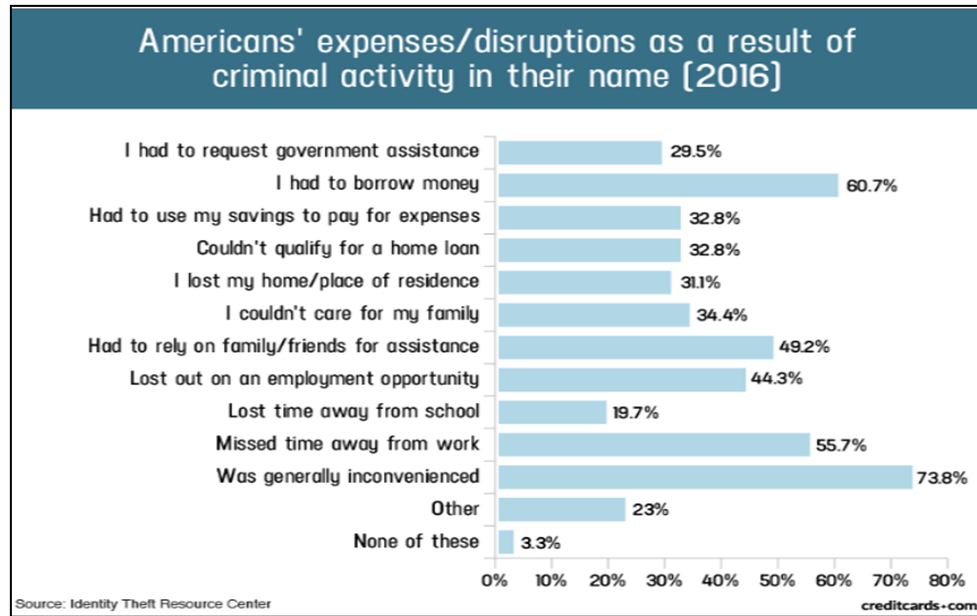
9 50. Thus, even if certain information was not purportedly involved in the
10 Data Breach, the unauthorized parties could use Plaintiff’s and Class Members’
11 Private Information to access accounts, including, but not limited to, email accounts
12 and financial accounts, to engage in a wide variety of fraudulent activity against
13 Plaintiff and Class Members.

14 51. For these reasons, the FTC recommends that identity theft victims take
15 several time-consuming steps to protect their personal and financial information after
16 a data breach, including contacting one of the credit bureaus to place a fraud alert on
17 their account (and an extended fraud alert that lasts for 7 years if someone steals the
18 victim’s identity), reviewing their credit reports, contacting companies to remove
19 fraudulent charges from their accounts, placing a freeze on their credit, and correcting
20 their credit reports.³ However, these steps do not guarantee protection from identity
21 theft but can only mitigate identity theft’s long-lasting negative impacts.

22 52. Identity thieves can also use stolen personal information such as Social
23 Security numbers for a variety of crimes, including medical identity theft, credit card
24 fraud, phone or utilities fraud, bank fraud, to obtain a driver’s license or official
25 identification card in the victim’s name but with the thief’s picture, to obtain
26 government benefits, or to file a fraudulent tax return using the victim’s information.

27
28 ³ See *IdentityTheft.gov*, Federal Trade Commission, *available at*
<https://www.identitytheft.gov/Steps> (last visited April 10, 2024).

53. In fact, a study by the Identity Theft Resource Center⁴ shows the multitude of harms caused by fraudulent use of PII:



54. The ramifications of Defendant's failure to keep its customers' and employees' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

55. The value of PII is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

56. PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

57. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

⁴ Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), available at <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/> (last visited on April 10, 2024).

Plaintiff's and Class Members' Damages

58. At some point prior to December 19, 2023, Defendant collected, obtained, and/or maintained substantial amounts of Plaintiff's personal information in its networks or systems, including PII, such as passport number, driver's license number, federal/state identification card number, tax identification number, social security and/or financial account information, and other information such as phone number, address, and email address.

59. On or about February 2, 2024, Plaintiff Kisling received notice from Defendant alerting her that her Private Information had been accessed and obtained by unauthorized actor through the Data Breach.

60. The notice letter offered Plaintiff only 12 months of credit monitoring services and an insurance policy – an insufficient remedy considering Plaintiff will now experience a lifetime of increased risk of identity theft.

61. Plaintiff suffered actual injury in the form of invasion of privacy and time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud, receiving multiple calls related to credit repair and loans following the data breach, suffering damage to her credit rating, and freezing her credit in order to mitigate further damages resulting from the Data Breach.

62. Plaintiff suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

63. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that was entrusted to Defendant and which was compromised in, and as a result of, the Data Breach.

64. Plaintiff suffered imminent and continuing impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

1 65. Plaintiff has a continuing interest in ensuring that her Private
2 Information, which remains in the possession of Defendant, is protected and
3 safeguarded from future breaches.

4 66. As a result of the Data Breach, Plaintiff made reasonable efforts to
5 mitigate the impact of the Data Breach, including but not limited to researching the
6 Data Breach, reviewing financial accounts for any indications of actual or attempted
7 identity theft or fraud, and researching the credit monitoring offered by Defendant.
8 Plaintiff has already spent several hours dealing with the Data Breach, valuable time
9 she otherwise would have spent on other activities.

10 67. As a result of the Data Breach, Plaintiff has suffered anxiety as a result
11 of the release of her Private Information, which she believed would be protected from
12 unauthorized access and disclosure. These feelings include anxiety about
13 unauthorized parties viewing, selling, and/or using her PII for purposes of committing
14 cyber and other crimes against her including, but not limited to, fraud and identity
15 theft. Plaintiff is very concerned about this increased, substantial, and continuing risk,
16 as well as the consequences that identity theft and fraud resulting from the Data
17 Breach would have on her life.

18 68. Plaintiff also suffered actual injury from having her Private Information
19 compromised as a result of the Data Breach in the form of (a) damage to and
20 diminution in the value of her PII, a form of property that Defendant obtained from
21 Plaintiff; (b) violation of her privacy rights; and (c) present, imminent, and impending
22 injury arising from the increased risk of identity theft, and fraud she now faces.

23 69. As a result of the Data Breach, Plaintiff anticipates spending
24 considerable time and money on an ongoing basis to try to mitigate and address the
25 many harms caused by the Data Breach.

26 70. In sum, Plaintiff and Class Members have been damaged by the
27 compromise of their Private Information in the Data Breach.

28 71. Plaintiff and Class Members entrusted their Private Information to

1 Defendant in order to receive Defendant's services.

2 72. Their Private Information was subsequently compromised as a direct and
3 proximate result of the Data Breach, which Data Breach resulted from Defendant's
4 inadequate data security practices.

5 73. As a direct and proximate result of Defendant's actions and omissions,
6 Plaintiff and Class Members have been harmed and are at an imminent, immediate,
7 and continuing increased risk of harm, including but not limited to, loans opened in
8 their names, tax returns filed in their names, utility bills opened in their names, credit
9 card accounts opened in their names, and other forms of identity theft.

10 74. Further, and as set forth above, as a direct and proximate result of
11 Defendant's conduct, Plaintiff and Class Members have also been forced to take the
12 time and effort to mitigate the actual and potential impact of the data breach on their
13 everyday lives, including placing "freezes" and "alerts" with credit reporting
14 agencies, contacting their financial institutions, closing or modifying financial
15 accounts, and closely reviewing and monitoring bank accounts and credit reports for
16 unauthorized activity for years to come.

17 75. Plaintiff and Class Members may also incur out-of-pocket costs for
18 protective measures such as credit monitoring fees, credit report fees, credit freeze
19 fees, and similar costs directly or indirectly related to the Data Breach.

20 76. Plaintiff and Class Members also face a substantial risk of being targeted
21 in future phishing, data intrusion, and other illegal schemes through the misuse of
22 their Private Information, since potential fraudsters will likely use such Private
23 Information to carry out such targeted schemes against Plaintiff and Class Members.

24 77. The Private Information maintained by and stolen from Defendant's
25 systems, combined with publicly available information, allows nefarious actors to
26 assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to
27 carry out targeted fraudulent schemes against Plaintiff and Class Members.

28 78. Plaintiff and Class Members also lost the benefit of the bargain they

made with the Defendant. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price paid by Plaintiff and Class Members (or, in some cases, on their behalf) to Defendant was intended to be used by Defendant to fund adequate security of Defendant's system and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive the benefit of the bargain.

79. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁵ In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to \$50 a year.⁶

80. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

81. Finally, Plaintiff and Class Members have suffered or will suffer actual

⁵ See <https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion>. (last visited on April 10, 2024).

⁶ *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, <https://computermobilepanel.nielsen.com/ui/US/en/faen.html> (last visited April 10, 2024).

injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

- a. Monitoring for and discovering fraudulent charges;
- b. Canceling and reissuing credit and debit cards;
- c. Addressing their inability to withdraw funds linked to compromised accounts;
- d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- f. Contacting financial institutions and closing or modifying financial accounts;
- g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
- i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

82. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendant, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal information of its customers and employees is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

83. As a direct and proximate result of Defendant's actions and inactions,

1 Plaintiff and Class Members have suffered a loss of privacy and have suffered
2 cognizable harm, including an imminent and substantial future risk of harm, in the
3 forms set forth above.

4 **CLASS ACTION ALLEGATIONS**

5 84. Plaintiff brings this action individually and on behalf of all other persons
6 similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1),
7 23(b)(2), and 23(b)(3).

8 85. Specifically, Plaintiff proposes the following Nationwide Class, subject
9 to amendment as appropriate:

10 All individuals whose Private Information was compromised in
11 the Data Breach which Defendant provided notice of on or
around February 2, 2024.

12 86. Excluded from the Class are Defendant and its parents or subsidiaries,
13 any entities in which it has a controlling interest, as well as its officers, directors,
14 affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also
15 excluded is any Judge to whom this case is assigned as well as their judicial staff and
16 immediate family members.

17 87. Plaintiff reserves the right to modify or amend the definition of the
18 proposed Class before the Court determines whether certification is appropriate.

19 88. The proposed Class meets the criteria for certification under Fed. R. Civ.
20 P. 23(a), (b)(2), and (b)(3).

21 89. Numerosity – The Class Members are so numerous that joinder of all
22 members is impracticable. Though the exact number and identities of Class Members
23 are unknown at this time, based on information and belief, the Class consists of at
24 least 27,746 current and former customers and employees of Sage Home Loans
25 whose data was compromised in the Data Breach. The identities of Class Members
26 are ascertainable through Defendant's records, Class Members' records, publication
27 notice, self-identification, and other means.

90. Commonality – There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members.

These common questions of law and fact include, without limitation:

- a. Whether Defendant engaged in the conduct alleged herein;
- b. Whether Defendant’s conduct violated the FTCA;
- c. When Defendant learned of the Data Breach;
- d. Whether Defendant’s response to the Data Breach was adequate;
- e. Whether Defendant unlawfully lost or disclosed Plaintiff’s and Class Members’ Private Information;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- g. Whether Defendant’s data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether Defendant’s data security systems prior to and during the Data Breach were consistent with industry standards;
- i. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- j. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- k. Whether hackers obtained Class Members’ Private Information via the Data Breach;
- l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class

Members;

- n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;
- p. Whether Defendant's conduct was negligent;
- q. Whether Defendant was unjustly enriched;
- r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

91. Typicality – Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Sage Home Loans. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff individually. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

92. Adequacy of Representation – Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

93. Superiority – A Class action is superior to other available methods for

1 the fair and efficient adjudication of this controversy and no unusual difficulties are
2 likely to be encountered in the management of this class action. Class treatment of
3 common questions of law and fact is superior to multiple individual actions or
4 piecemeal litigation. Absent a Class action, most Class Members would likely find
5 that the cost of litigating their individual claims is prohibitively high and would
6 therefore have no effective remedy. The prosecution of separate actions by individual
7 Class Members would create a risk of inconsistent or varying adjudications with
8 respect to individual Class Members, which would establish incompatible standards
9 of conduct for Defendant. In contrast, conducting this action as a class action presents
10 far fewer management difficulties, conserves judicial resources and the parties'
11 resources, and protects the rights of each Class Member.

12 94. Finally, all members of the proposed Class are readily ascertainable.
13 Defendant has access to the names and addresses and/or email addresses of Class
14 Members affected by the Data Breach. Class Members have already been
15 preliminarily identified and sent notice of the Data Breach by Defendant.

16 **CLAIMS FOR RELIEF**

17 **FIRST CAUSE OF ACTION**

18 **NEGLIGENCE**

19 95. Plaintiff restates and realleges all of the allegations in every preceding
20 paragraph as if fully set forth herein.

21 96. Defendant knowingly collected, came into possession of, and maintained
22 Plaintiff's and Class Members' Private Information, and had a duty to exercise
23 reasonable care in safeguarding, securing, and protecting such Information from
24 being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

25 97. Defendant knew or should have known of the risks inherent in collecting
26 the Private Information of Plaintiff and Class Members and the importance of
27 adequate security. Defendant was on notice because, on information and belief, it
28 knew or should have known that it would be an attractive target for cyberattacks.

98. Defendant owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Defendant's duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;
- d. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- e. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

99. Defendant's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

100. Defendant's duty also arose because Defendant was bound by industry standards to protect customers' and employees' confidential Private Information.

101. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Defendant owed them a duty of care to not subject them to an unreasonable risk of harm.

102. Defendant, through its actions and/or omissions, breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's

possession.

103. Defendant, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

104. Defendant, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

105. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to comply with the FTCA; and
- f. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

106. Defendant was fully capable of preventing the Data Breach, compromising its systems (and the Private Information that it stored on them) from attack. As an entity in the business of providing loans and handling Private Information, Defendant knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. Defendant

1 thus failed to take reasonable measures to secure its system, leaving it vulnerable to a
2 breach.

3 107. Defendant's breach of duties owed to Plaintiff and Class Members
4 caused Plaintiff's and Class Members' Private Information to be compromised,
5 exfiltrated, and/or misused, as alleged herein.

6 108. As a result of Defendant's ongoing failure to notify Plaintiff and Class
7 Members regarding exactly what Private Information has been compromised,
8 Plaintiff and Class Members have been unable to take the necessary precautions to
9 prevent future fraud and mitigate damages.

10 109. Defendant's breaches of duty also caused a substantial, imminent risk to
11 Plaintiff and Class Members of identity theft, loss of control over their Private
12 Information, and/or loss of time and money to monitor their accounts for fraud.

13 110. As a result of Defendant's negligence in breach of its duties owed to
14 Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent
15 harm in that their Private Information, which is still in the possession of third parties,
16 will be used for fraudulent purposes.

17 111. As a direct and proximate result of Defendant's negligent conduct,
18 Plaintiff and Class Members have suffered damages as a result of Defendant's
19 negligence, including actual and concrete injuries and will suffer additional injuries in
20 the future, including economic and non-economic damages from invasion of privacy,
21 costs related to mitigating the imminent risks of identity theft, time and effort related
22 to mitigating present and future harms, actual identity theft, the loss of the benefit of
23 bargained-for security practices that were not provided as represented, and the
24 diminution of value in their Private Information and PII.

25 112. The injury and harm that Plaintiff and Class Members suffered was
26 reasonably foreseeable.

27 113. Plaintiff and Class Members have suffered injury and are entitled to
28 damages in an amount to be proven at trial, including compensatory, punitive, and/or

nominal damages, and/or disgorgement or restitution.

114. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

SECOND CAUSE OF ACTION

NEGLIGENCE PER SE

115. Plaintiff restates and realleges the allegations in every preceding paragraph as if fully set forth herein.

116. Defendant's unreasonable data security measures constitute unfair or deceptive acts or practices in or affecting commerce in violation Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, it requires businesses to institute reasonable data security measures and breach notification procedures, which Defendant failed to do.

117. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect users' sensitive data. The FTC's complaint against Defendant also forms the basis of Defendant's duty.

118. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the sensitive nature and amount of data Defendant stored on their users and the foreseeable consequences of a Data Breach should Defendant fail to secure their systems or networks.

119. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

120. In addition, the California Consumer Privacy Act (“CCPA”), Cal. Civ. Code §§ 1798.100, et seq. requires “[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.” 1798.81.5(c).

121. Defendant violated the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff’s and Class members’ Private Information and PII. Defendant failed to implement reasonable security procedures and practices to prevent an attack on its servers or systems by hackers and to prevent unauthorized access and exfiltration of Plaintiff’s and Class members’ PII as a result of the Data Breach.

122. Plaintiff and the Class are within the class of persons Section 5 of the FTC Act, the CCPA, and other similar state statutes, was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act. The CCPA, and other similar state statutes, was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

123. As a direct and proximate result of Defendant’s negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

THIRD CAUSE OF ACTION

UNJUST ENRICHMENT

124. Plaintiff restates and realleges the allegations in every preceding paragraph as if fully set forth herein.

125. This cause of action is pleaded in the alternative to Plaintiff’s second

1 cause of action above.

2 126. Plaintiff and Class Members conferred a benefit on Defendant by turning
3 over their valuable Private Information to Defendant with the understanding that the
4 benefits earned from possession and control thereof would be utilized, in part, to
5 provide adequate data security to protect such Private Information. Plaintiff and Class
6 Members did not receive such protection.

7 127. Defendant knew that Plaintiff and Class Members conferred a benefit
8 upon it and has accepted and retained that benefit by accepting and retaining the
9 Private Information entrusted to it. Defendant profited from Plaintiff's retained data
10 and used Plaintiff's and Class Members' Private Information for business purposes.

11 128. Defendant failed to secure Plaintiff's and Class Members' Private
12 Information and, therefore, did not fully compensate Plaintiff or Class Members for
13 the value that their Private Information provided.

14 129. Defendant acquired the Private Information through inequitable record
15 retention as it failed to disclose the inadequate data security practices previously
16 alleged.

17 130. If Plaintiff and Class Members had known that Defendant would not use
18 adequate data security practices, procedures, and protocols to adequately monitor,
19 supervise, and secure their Private Information, they would not have entrusted their
20 Private Information with Defendant or become employees and/or customers of
21 Defendant.

22 131. Plaintiff and Class Members have no adequate remedy at law.

23 132. Under the circumstances, it would be unjust for Defendant to be
24 permitted to retain any of the benefits that Plaintiff and Class Members conferred
25 upon it.

26 133. As a direct and proximate result of Defendant's conduct, Plaintiff and
27 Class Members have suffered and will suffer injury, including but not limited to: (i)
28 invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished

1 value of Private Information; (iv) lost time and opportunity costs associated with
2 attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit
3 of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the
4 actual consequences of the Data Breach; (vii) experiencing an increase in spam calls,
5 texts, and/or emails; (viii) dissemination of their Private Information on the dark web;
6 (ix) statutory damages; (x) nominal damages; and (xi) the continued and certainly
7 increased risk to their Private Information, which: (a) remains unencrypted and
8 available for unauthorized third parties to access and abuse; and (b) remains backed
9 up in Defendant's possession and subject to further unauthorized disclosures so long
10 as Defendant fails to undertake appropriate and adequate measures to protect the
11 Private Information.

12 134. Plaintiff and Class Members are entitled to full refunds, restitution,
13 and/or damages from Defendant and/or an order proportionally disgorging all profits,
14 benefits, and other compensation obtained by Defendant from its wrongful conduct.
15 This can be accomplished by establishing a constructive trust from which the Plaintiff
16 and Class Members may seek restitution or compensation.

17 **FOURTH CAUSE OF ACTION**

18 **DECLARATORY AND INJUNCTIVE RELIEF**

19 135. Plaintiff restates and realleges the allegations in every preceding
20 paragraph as if fully set forth herein.

21 136. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, et seq., this
22 Court is authorized to enter a judgment declaring the rights and legal relations of the
23 parties and grant further necessary relief. Furthermore, the Court has broad authority
24 to restrain acts, such as those alleged herein, which are tortious, and which violate the
25 terms of the federal and state statutes described above.

26 137. An actual controversy has arisen in the wake of the Data Breach at issue
27 regarding Defendant's common law and other duties to act reasonably with respect
28 to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendant's

1 actions in this respect were inadequate and unreasonable and, upon information and
2 belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class
3 continue to suffer injury due to the continued and ongoing threat of additional fraud
4 against them or on their accounts.

5 138. Pursuant to its authority under the Declaratory Judgment Act, this Court
6 should enter a judgment declaring, among other things, the following:

7 a. Defendant owed, and continue to owe a legal duty to secure the
8 sensitive personal information with which they are entrusted, specifically including
9 information obtained from its customers, and to notify impacted individuals of the
10 Data Breach under the common law, Section 5 of the FTC Act;

11 b. Defendant breached, and continue to breach, their legal duty by
12 failing to employ reasonable measures to secure their customers' personal
13 information; and,

14 c. Defendant's breach of their legal duty continues to cause harm to
15 Plaintiff and the Class.

16 139. The Court should also issue corresponding injunctive relief requiring
17 Defendant to employ adequate security protocols consistent with industry standards
18 to protect its users' data.

19 140. If an injunction is not issued, Plaintiff and the Class will suffer
20 irreparable injury and lack an adequate legal remedy in the event of another breach of
21 Defendant's data systems. If another breach of Defendant's data systems occurs,
22 Plaintiff and the Class will not have an adequate remedy at law because many of the
23 resulting injuries are not readily quantified in full and they will be forced to bring
24 multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while
25 warranted to compensate Plaintiff and the Class for their out-of-pocket and other
26 damages that are legally quantifiable and provable, do not cover the full extent of
27 injuries suffered by Plaintiff and the Class, which include monetary damages that are
28 not legally quantifiable or provable.

1 141. The hardship to Plaintiff and the Class if an injunction does not issue
2 exceeds the hardship to Defendant if an injunction is issued.

3 142. Issuance of the requested injunction will not disserve the public interest.
4 To the contrary, such an injunction would benefit the public by preventing another
5 data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and
6 the public at large.

7 **PRAYER FOR RELIEF**

8 WHEREFORE, Plaintiff, on behalf of herself and the Class described above,
9 seeks the following relief:

- 10 a. An order certifying this action as a Class action, defining the Class as
11 requested herein, appointing the undersigned as Class counsel, and finding
12 that Plaintiff is a proper and adequate representative of the Class requested
13 herein;
- 14 b. Judgment in favor of Plaintiff and Class Members awarding them
15 appropriate monetary relief, including actual damages, statutory damages,
16 equitable relief, restitution, disgorgement, and statutory costs;
- 17 c. A declaratory judgment in favor of Plaintiff and the Class;
- 18 d. An order providing injunctive relief and other equitable relief as necessary
19 to protect the interests of Plaintiff and the Class as requested herein;
- 20 e. An order requiring Defendant to pay the costs involved in notifying Class
21 Members about the judgment and administering the claims process;
- 22 f. An order requiring Defendant to implement enhanced data security
23 measures in order to better protect the PII in its possession and control;
- 24 g. A judgment in favor of Plaintiff and Class Members awarding them
25 prejudgment and post-judgment interest;
- 26 h. An award of reasonable attorneys' fees, costs, and expenses as allowable by
27 law; and
- 28 i. Any such other and further relief this Court may deem just and proper.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

